อาชญากรคอมพิวเตอร์ : การทำลายและความหายนะ

พาท่านไปรู้จักกับอาชญากรคอมพิวเตอร์ ตัวการร้ายที่คอยฉกฉวยข้อมูลเพื่อประโยชน์ส่วนตนจนทำให้วงการคอมพิวเตอร์ต้องปั่นป่วน

ด้วยความแตกต่างในตัวของคนแต่ละคน จึงทำให้โลกนี้มีสีสัน มีชีวิตชีวา และมีความสับสนวุ่นวาย ในบรรดาผู้ที่ก่อให้เกิดความวุ่นวายเหล่านั้น ส่วนใหญ่มักเกิดจากคำว่า "ไม่พอดี" ในความไม่พอดีของมนุษย์จึงทำให้มีมนุษย์ที่ฉลาดน้อยถูกเอาเปรียบจากมนุษย์ที่ฉลาดมาก การเอาเปรียบโดยวิธีการทุจริต ฉ้อฉล คดโกงมีในทุกแขนงอาชีพ ในแวดวงคอมพิวเตอร์เหตุการณ์วุ่นวายมักเกิดจากมนุษย์ฉลาดมากที่ไม่รู้จักคำว่าพอดี ดังนั้น จึงมีอาชญากรคอมพิวเตอร์เกิดขึ้น

อาชญากรคอมพิวเตอร์ คืออะไร ?

อาชญากรคอมพิวเตอร์ คำนี้ค่อนข้างยาว ดังนั้น เราจึงค่อนข้างจะคุ้นเคยกับคำว่า แฮกเกอร์ (Hacker) ซึ่งแต่เดิมเป็นบุคคลหรือกลุ่มบุคคลที่ชอบละเมิดสิทธิต่อบุคคลอื่น เจาะฐานข้อมูลหรือระบบสารสนเทศเพียงเพื่อการเรียนรู้ระบบหรือกลไกทางเทคนิคแต่เพียงอย่างเดียว ในปัจจุบันพฤติกรรมของแฮกเกอร์ได้แปรเปลี่ยนไป เกิดพฤติกรรมการทำลายล้างข้อมูล จนผู้ที่อยู่ในวงการคอมพิวเตอร์เรียกพวกทำลายล้างข้อมูลเหล่านี้ว่าเป็นพวกแครกเกอร์ (Cracker) ซึ่งความแตกต่างของทั้งสองคำนิยามนี้อยู่ที่เป้าหมายในการจารกรรมข้อมูล จึงมีผู้นิยามคำว่าแฮกเกอร์และแครกเกอร์ไว้ดังนี้

Hacker หมายถึง บุคคลที่เป็นอัจฉริยะมีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบรักษาความปลอดภัยของคอมพิวเตอร์ได้

Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดีจนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบไฟล์ หรือทำให้เครื่องคอมพิวเตอร์เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

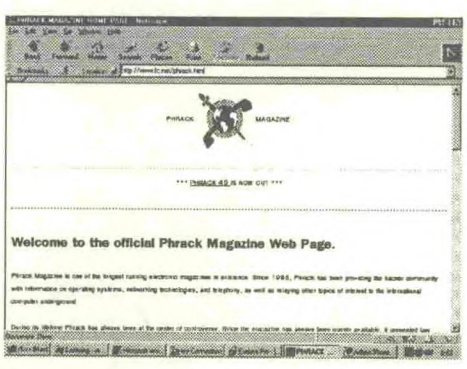
เท่าที่อ่านพบในนิตยสารหรือสื่อสิ่งพิมพ์ต่าง ๆ ในบ้านเรา พบว่านิยมใช้คำว่าแฮกเกอร์ ซึ่งต่อไปนี้คุณก็คงเข้าใจและอาจจำง่าย ๆ ว่าแฮกเกอร์เป็นพวกซุกซนลองของ ไม่ร้ายแรงมากเหมือนกับพวกแครกเกอร์ที่รุนแรงกว่าและก่อให้เกิดความเสียหายอย่างที่กล่าวมา ซึ่งเราเรียกคนจำพวกหลังนี้ว่า "อาชญากรคอมพิวเตอร์" นั่นเอง และอาชญากรคอมพิวเตอร์ ถ้าจะแปลให้เข้าใจง่าย ๆ ก็คือ ผู้ที่กระทำผิดกฎหมายเกี่ยวกับคอมพิวเตอร์ ก็คือ การกระทำใด ๆ ที่เกี่ยวกับการใช้การเข้าถึงข้อมูล โดยที่ผู้กระทำไม่ได้รับอนุญาต แม้ไม่ถึงกับเป็นการกระทำที่ผิดกฎหมาย แต่เป็นการกระทำที่ผิดระเบียบกฎเกณฑ์ของการใช้คอมพิวเตอร์นั้น ๆ

ทำไมถึงต้องโทษเป็นอาชญากรคอมพิวเตอร์

การแบ่งแยกพวกที่กระทำผิดที่สมควรให้ต้องโทษเป็นอาชญากรคอมพิวเตอร์ (Computer Criminal) แบ่งออกได้เป็น 7 พวก ได้แก่ พวกหัดใหม่ พวกวิกล-จริต พวกมืออาชีพ พวกหัวพัฒนา พวกช่างคิดช่างฝัน พวกแฮกเกอร์/แครกเกอร์ และพวกที่ประกอบอาชญากรรมหรือกลุ่มมิจฉาชีพตัวจริงนั่นเอง

ซึ่งจริง ๆ แล้วหากจะคาดโทษที่วัดจากความสูญเสียแล้ว พวกอาชญากรคอมพิวเตอร์น่าจะมีมากกว่า 7 พวกที่กล่าวมา ยกตัวอย่างเช่น มีเจ้าหน้าที่ดูแลระบบคอมพิวเตอร์ของบริษัทหนึ่ง ถูกกลั่นแกล้งจนไม่สามารถจะทำงานในบริษัทนั้นต่อไปได้ จึงตัดสินใจลาออก วันสุดท้ายก่อนออกจากบริษัท พนักงานคนนั้นก็ได้ลบข้อมูลสำคัญของบริษัท ทำให้บริษัทนั้นได้รับความเสียหายเป็นอย่างมาก ในกรณีนี้ก็น่าจะเข้าข่ายอาชญากรคอมพิวเตอร์และสมควรที่จะจัดเข้ากลุ่มใหม่ให้ชื่อว่า พวกผีพยาบาท ผีอาฆาต ผีจองเวร ผี... ซึ่งก็สามารถตีความไปได้หลาย ๆ ประเด็น ดังนั้นข้อกฎหมายจะต้องระบุให้แน่ชัดและรัดกุมให้มากกว่านี้ เพราะเทคโนโลยีคอมพิวเตอร์มีการเปลี่ยนแปลงไปได้เร็วที่สุด

การเสาะหาแหล่งข้อมูลเพื่อเทคนิคการเป็นอาชญากรคอมพิวเตอร์ หากรู้แหล่งข้อมูลก็ช่างจะเป็นเรื่องง่ายดายเสียเหลือเกิน สำหรับผู้ที่ใช้โปรแกรมเวบบราวเซอร์และไปยังเวบไซท์สำหรับการค้นหาข้อมูล (Search Engine) ป้อนคำที่มีความหมายเกี่ยวข้องกับการจารกรรมหรือการรักษาความปลอดภัย เช่น Hacker, Cracker, secutiry หรือจะติดตามอ่านจากวารสารชื่อ Phrack สำหรับอาชญากรคอมพิวเตอร์มือใหม่ ที่รวบรวมข้อมูลเทคนิคต่าง ๆ เอาไว้ สนใจสามารถแวะดูที่ http://www.fc.net/phrack.html ขอให้อ่านเพื่อประเทืองปัญญา แต่ขอความกรุณาว่าอย่านำมาใช้ในทางที่ผิดก็แล้วกัน



จากข่าวคราวตามสื่อต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ เราท่านอาจเคยได้ยินคดีความในต่างประเทศเกี่ยวกับการใช้อินเทอร์เน็ตในการเจาะข้อมูลในองค์กรธุรกิจและรัฐบาล เช่นในกรณีการลักลอบเจาะฐานข้อมูลที่เก็บรหัสบัตร-เครดิตของลูกค้าธนาคารและทำการโอนเงินเข้าบัญชีของเหล่าอาชญากรคอมพิวเตอร์ การแอบเจาะข้อมูลสำคัญของทางรัฐบาล สร้างความสั่นคลอนให้กับเสถียรภาพความมั่นคงของภาครัฐ การแอบเจาะข้อมูลที่เป็นความลับขององค์กรธุรกิจและนำไปขายให้กับอีกองค์กรหนึ่งที่เป็นคู่แข่ง เหล่านี้เป็นต้น ซึ่งอาชญากรในบางกรณีเราอาจจะทราบถึงการสืบหาและจับกุมได้ในเวลาต่อมา แต่ในบางกรณีอาจจะยังลอยนวลอยู่...

การละเมิดลิขสิทธิ์ในไทยก็น่าเป็นห่วง

การก่ออาชญากรรมทางด้านคอมพิวเตอร์นั้นยังไม่มีมากนักเหมือนในต่างประเทศ จะมีแต่ก็โดนหลอกให้เสียเงินโดยรู้เท่าไม่ถึงการณ์จากการใช้อินเทอร์เน็ต แต่สิ่งที่พบมากที่สุดในประเทศไทยก็คือ การละเมิดลิขสิทธิ์ซอฟต์แวร์ ซึ่งก็เป็นที่รู้ ๆ กันว่าซอฟต์แวร์ที่มีประสิทธิภาพและนิยมใช้มักเป็นซอฟต์แวร์นำเข้าจากต่างประเทศ ส่วนซอฟต์แวร์ที่จะต้องใช้เฉพาะงานจริง ๆ เป็นซอฟต์แวร์ที่ผลิตในประเทศไทย ส่วนฟรีแวร์ในไทยยังมีไม่มากนัก ยกตัวอย่างเช่น เวิร์ดโปรเซสเซอร์ RW, CW, RAMA Word เป็นต้น

การซื้อซอฟต์แวร์มาใช้ด้วยราคาสูง กับการซื้อซอฟต์แวร์ที่ก๊อบปี้เถื่อนมาจากแหล่งใหญ่ ที่เรารู้ ๆ กันอย่างหลังได้รับความนิยมมากกว่า ดังนั้นบริษัทที่พัฒนาซอฟต์แวร์จึงแก้เผ็ดผู้ที่ชอบละเมิดลิขสิทธิ โดยการเขียนโปรแกรมก่อกวนทำลายล้างข้อมูล นี่ก็คือเหตุผลที่ทำให้เกิดไวรัสคอมพิวเตอร์ ปัญหาที่แก้ไม่ตกอีกปัญหาหนึ่ง

สถานะการณ์คอมพิวเตอร์ในไทยหลังจากการมาเยือนของ "บิล คลินตัน" ประธานาธิบดีของสหรัฐอเมริกาที่ผ่านมาเมื่อเร็ว ๆ นี้ พกพาข้อกำหนดที่ทำให้ซอฟต์แวร์ต่างประเทศซึ่งแต่เดิมราคาสูง มีเค้าปรับราคาลดลง โดยข้อกำหนดเขตปลอดภาษี ITA (Information Technology Agreement) ที่จะส่งผลกระทบถึงการพัฒนาซอฟต์แวร์ในประเทศ เพราะข้อกำหนดดังกล่าวทำให้ราคาซอฟต์แวร์จากต่างประเทศมีราคาถูกลง ข้อมูลโดยประมาณการถึงมูลค่าตลาดซอฟต์แวร์ในไทยปี 2540 จะมีมูลค่าถึง 3,000 ล้านบาท และคาดว่าจะมีการขยายตัวใน

ปี 2542 จะเพิ่มขึ้นเป็น 7,000 - 8,000 ล้านบาท โดยซอฟต์แวร์ที่คนไทยผลิตขึ้นมามีมูลค่าในตลาดมากที่สุดเป็นซอฟต์แวร์ทางด้านบัญชี มีมูลค่าประมาณ 260 ล้านบาท ในปี 2539 และจะเพิ่มเป็น 364 ล้านบาทในปี 2540 นี้

ดังนั้น แนวทางในการแก้ไขส่วนหนึ่งจากภาครัฐบาล โดยความร่วมมือของเนคเทค และBOI ได้ร่วมกันทำโครงการศูนย์อุตสาหกรรมซอฟต์แวร์หรือซอฟต์แวร์ปาร์ค (Software Park) จะเป็นสถานที่บริษัทนักพัฒนาซอฟต์แวร์มาอยู่รวมกันในอาคารสูงประมาณ 20 ชั้น ในวงเงินอนุมัติเบื้องต้น 1,300 - 1,500 ล้านบาท เพื่อระดมความคิดให้มีการแข่งขันและก่อให้การพัฒนาจากภูมิปัญญาของคนไทย ไม่ต้องไปพึ่งพาซอฟต์แวร์ต่างประเทศ

ตำรวจไทยเตรียมรับอาชญากรคอมพิวเตอร์

กรมตำรวจไทยก็ได้หามาตรการเพื่อรับมือกับเหล่าอาชญากรคอมพิวเตอร์ที่จะมาในรูปแบบต่าง ๆ โดยระดมจัดสัมมนาเรื่อง "อาชญากรคอมพิวเตอร์" ให้กับนายตำรวจจำนวน 80 นาย จากแหล่งข่าวกล่าวว่าได้รับความร่วมมืออนุเคราะห์วิทยากรผู้บรรยาย บินมาจากมหาวิทยาลัยมิชิแกนสเตท สหรัฐอเมริกา ซึ่งเป็นสถาบันที่ทำการฝึกอบรมให้กับเอฟบีไอ และนอกจากนี้ทางกรมตำรวจมีการร่วมมือกับตำรวจสากล (Interpol) เพื่อหาเบาะแสคดีสำคัญที่เป็นคดีระหว่างประเทศ โดยมีศูนย์กลางข้อมูลที่ติดต่อผ่านระบบคอมพิวเตอร์ออนไลน์อยู่ที่ประเทศสิงคโปร์ และแผนการต่อไปที่จะดำเนินการก็คือการตั้งศูนย์กลางในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ในภูมิภาคนี้ โดยเตรียมที่จะนำเสนอในการประชุมตำรวจอาเซียน (Asean Pol) ในครั้งต่อไป

บทสรุป

ความรู้ความสามารถหากใช้ให้ถูกทางก็จะเป็นสิ่งสร้างสรรค์จรรโลงสังคม แต่หากใช้ในทางที่ผิด ก็เป็นอาวุธร้ายที่ใช้ประหัดประหารผู้อื่น ดังนั้นการแก้ปัญหาอาชญากรคอมพิวเตอร์ ควรจะเริ่มต้นตั้งแต่การปลูกฝังให้ค่านิยม และการสร้างคุณธรรมให้กับบุคลากรทางด้านคอมพิวเตอร์ พร้อมทั้งการตั้งกฎหมายออกกฎระเบียบควบคุมและมีมาตรการที่เด็ดขาดและเข้มงวด เพราะกฎหมายมีความศักดิ์สิทธิ์ อาชญากรที่ทำผิด...ต้องจับเข้าคุกซะให้เข็ด